

O que são cookies do navegador e como os atacantes os exploram?

Resposta curta: Os cookies são pequenos fragmentos de dados que um site armazena no seu navegador, e alguns deles são cookies de autenticação que mantêm a sua sessão iniciada. Roubar esses cookies é funcionalmente equivalente a roubar uma sessão ativa — o atacante pode carregá-los no seu próprio navegador e passar por si.

Nem todos os cookies têm a mesma importância

- **Cookies de preferências** — idioma, tema, esquema. Valor reduzido.
- **Cookies de análise (analytics)** — medição de utilização. Valor reduzido.
- **Cookies de autenticação / sessão** — comprovam que a sessão está iniciada. **Valor elevado.**

Os atacantes preocupam-se quase exclusivamente com a terceira categoria.

Por que razão o roubo de cookies é eficaz

Um cookie de autenticação roubado normalmente não despoleta um evento de início de sessão, um pedido de palavra-passe, ou um desafio de MFA. A sessão já existe; o atacante está simplesmente a apresentar a prova disso. Do ponto de vista da aplicação, isto parece atividade normal e contínua.

Os navegadores armazenam os cookies em localizações de ficheiros conhecidas e previsíveis em todos os sistemas operativos, pelo que ferramentas automatizadas conseguem localizá-los sem ter qualquer conhecimento sobre a máquina em causa.

Por que razão o navegador é um ponto focal

O navegador reúne num só local os cookies, palavras-passe guardadas, tokens OAuth e o histórico, o que o torna o alvo de identidade mais rico num único ponto na maioria dos terminais. A Cyber Crucible observou isto diretamente: a partir do 4.º trimestre de 2023, as respostas automatizadas contra atividade do Chrome, Edge e Chromium aumentaram de zero para milhares, com CVEs relacionados publicados posteriormente pela Google e pela Microsoft.

Proteção

O armazenamento de credenciais do navegador é uma das localizações de identidade protegidas. Um processo que tente lê-lo é avaliado em contexto — um navegador comprometido é tratado de forma muito diferente de um navegador íntegro, e em nenhum dos casos um pedido excessivo recebe o cookie real.

Revision #1

Created 2026-07-24 05:42:08 UTC by Dennis Underwood

Updated 2026-07-24 05:42:08 UTC by Dennis Underwood